2/22/24, 9:51 AM quadratic\_sieve

```
In [26]:
          import numpy as np
          import math116
          import sympy
 In [2]:
          \verb"a_1=124402475107436956653214995731541180380280997149369997221299"
          a\_2 = 199847229374817823695604940715369430085494552242478434608955
          a \ \ 3 = 220858176749437491899576629985186381333365508025928999995553
          a 4=227878773345183169438253920129201946121066699139046176529585
          a\_5 = 267490954776053814955799615403242750359670807241877604975611
          a\_6 = 324559476413609681306894328864179166726048737902962384692208
          a\_7 = 354138716512743098120402603091175713331952656954461941040433
          \texttt{a} \ \ 8 = 364993010783551085705959529753890281863717553767874470391160
          n = 1045592161748229528611072437202613436041386826857744222177653
 In [3]:
          a_1_2 = pow(a_1, 2, n)
          a_2_2=pow(a_2,2,n)
          a_3_2 = pow(a_3, 2, n)
          a_4_2 = pow(a_4, 2, n)
          a_5_2 = pow(a_5, 2, n)
          a_{6}^{2}=pow(a_{6},2,n)
          a_7_2 = pow(a_7, 2, n)
          a_8_2 = pow(a_8, 2, n)
In [20]:
          a_8_2
         298995840
Out[20]:
In [21]:
          a_1_2_a=np.array([6,3,0,2,0,0])
          a_2_2_a=np.array([6,1,2,1,2,2])
          a_3_2_a=np.array([5,0,1,2,0,0])
          a_4_2_a=np.array([0,0,2,1,0,0])
          a_5_2_a=np.array([3,3,3,2,0,2])
          a_6_2_a=np.array([7,1,3,3,1,1])
          a_7_2_a=np.array([2,1,2,1,1,1])
          a_8_2_a=np.array([7,3,1,0,3,1])
In [22]:
          a_1_mod=a_1_2_a%2
          a_2_mod=a_2_2_a%2
          a_3_mod=a_3_2_a%2
          a_4_mod=a_4_2_a%2
          a_5_mod=a_5_2_a%2
          a_6_mod=a_6_2_a%2
          a_7_mod=a_7_2_a%2
          a 8 mod=a 8 2 a%2
In [24]:
          mod_2_matrix=np.array([a_1_mod,a_2_mod,a_3_mod,a_4_mod,a_5_mod,a_6_mod,a_7_mod,a
In [25]:
          mod_2_matrix
Out[25]: array([[0, 1, 0, 0, 0, 0],
                 [0, 1, 0, 1, 0, 0],
                 [1, 0, 1, 0, 0, 0],
                 [0, 0, 0, 1, 0, 0],
                 [1, 1, 1, 0, 0, 0],
                 [1, 1, 1, 1, 1, 1],
                 [0, 1, 0, 1, 1, 1]
                 [1, 1, 1, 0, 1, 1]])
In [27]:
          M=sympy.Matrix(mod_2_matrix)
In [28]:
          M_rref=M.rref()
In [29]:
          M_rref
```

2/22/24, 9:51 AM quadratic\_sieve